## REMARKS

Reconsideration of the above-identified patent application in view of the amendments above and the remarks following is respectfully requested.

Claims 1-14 and 16-26 are in this case. Claims 20-22 have been rejected under § 101. Claims 1-14 and 16-22 have been rejected under § 103(a). Independent claims 1, 11, 16, 17 and 20 and dependent claims 6, 10, 14 and 22 have been amended.

Specifically:

The independent claims have been amended to clarify that the attempt to disassemble the suspicious data is an attempt to produce disassembled executable code, and that the subsequent steps of assigning and accumulating threat weights are conditional on the attempt to disassemble the suspicious data succeeding in producing disassembled executable code. Support for these amendments is found in the specification as filed at least on page 9 lines 16-17:

> Subsequent to disassembly, an instruction analyzer **405** is used to determine if the code is executable code and malicious. (emphasis added)

The amendment of claim 20 to overcome the rejection under § 101 is discussed below.

The labels of the elements recited in dependent claims 6, 10, 14 and 22 have been amended to be consistent with the parent claims of these dependent claims.

### § 101 Rejections

The Examiner has rejected claims 20-22 under § 101 as being directed to non-statutory subject matter. Specifically, the Examiner has pointed out that the three

elements recited in claim 20 are defined in the specification (page 5 line 28, page 8 line 26) as "software modules".

Therefore, claim 20 has been amended to recite the three elements as "a plurality of software modules" and to also recite a processor for executing the software modules. Support for the latter amendment is found in the above-identified patent application as filed at least in processor **201** of Figure 2.

**§ 103(a) Rejections – Radatti et al. '540 in view of Szor '290 and Schmall**

The Examiner has rejected claims 1, 3, 4, 10 and 20 under § 103(a) as being unpatentable over Radatti et al., US Patent No. 7,389,540 (henceforth, "Radatti et al. '540") in view of Szor, US Patent No. 7,293,290 (henceforth, "Szor '290") and Schmall, "Classification and identification of malicious code based on heuristic techniques utilizing Meta languages" (PhD thesis, 2003) (henceforth, "Schmall"). The Examiner's rejection is respectfully traversed.

Radatti et al. '540 teaches intercepting and examining code passing between components of a network. Szor '290 teaches looking for malicious executable code leaving a host computer **1** at a port **15** where outbound executable code is not expected, by looking for strings of known executable code in the data exiting port **15**.

Schmall teaches heuristic technology, for detecting malicious code, that includes disassembling the suspicious code and assigning and accumulating weights of disassembled instructions. The Examiner has proposed that it would be obvious to substitute Schmall's heuristic technology for the string matching of Szor '290.

In order for independent claims 1 and 20 to be unpatentable over Radatti et al. '540 in view of Szor '290 and Schmall, these references must teach or suggest every recited limitation. As the Board of Patent Appeal and Interferences has confirmed in *In re Wada and Murphy*, Appeal 2007-3733,

> When determining whether a claim is obvious, an examiner must make "a searching comparison of the claimed invention – *including all its limitations* – within the teaching of the prior art". *In re Orchiai*, 71 F.3d 1565, 1572 (Fed. Cir. 1995) (emphasis added). Thus, "Obviousness requires a suggestion of all limitations in a claim." *CFMT, Inc. v. Yieldup Intern. Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003) (citing *In re Royka*, 490 F.2d 981, 985 (CCPA 1974)).

In the present case, at least one limitation, recited in independent claims 1 and 20 as now amended, is neither taught nor hinted nor suggested by the prior art cited by the Examiner. This limitation is that the disassembling of the suspicious data is merely an *attempt* to disassemble the suspicious data, with the subsequent assigning and accumulating threat weights on the disassembling being contingent on the disassembling actually succeeding in producing disassembled executable code, without knowing in advance that the suspicious data in fact includes executable code. Schmall *assumes* that the input to his heuristic technology is known to be executable code, as is clear *e.g.* from the third paragraph on page 146:

> Heuristic scanning is similar to signature scanning, except that instead of looking for specific signatures, heuristic scanning involves looking for certain instructions within a program, most of which aren't found in typical application programs. (emphasis added)

(as opposed to looking for instructions within data generally), from the first paragraph on page 193:

> ...the heuristic detection methods/functionality for Visual Basic Script (VBS), Visual Basic for Applications (VBA), Motorola Mc680x0 assembly language and the x86 architecture based malicious codes have been extensively researched.

(connecting the heuristic technology with specific executable languages) and from the title of section 6.1 on page 219,

> Technical basis concept for the heuristic engine to detect script language based malicious code (emphasis added)

There is neither a hint nor a suggestion in the prior art cited by the Examiner of attempting disassembly in order to find out whether suspicious data, that is not known

*a priori* to include executable code, in fact does includes executable code. Indeed, as best understood, it is precisely the uncertainty of Szor '290 as to whether the data leaving host computer **1** at port **15** includes executable code that led Szor '290 to prefer signature scanning over heuristic scanning. Any assertion to the contrary by the Examiner constitutes impermissible hindsight.

It follows that independent claims 1 and 20 are allowable in their present form over the prior art cited by the Examiner. It further follows that claims 3, 4 and 10 that depend from claim 1 also are allowable.

**§ 103(a) Rejections – Radatti et al. '540 in view of Szor '290 and Schmall and further in view of Muttik '780**

The Examiner has rejected claims 11, 16 and 17 under § 103(a) as being unpatentable over Radatti et al. '540 in view of Szor '290 and Schmall and further in view of Muttik, US Patent No. 6,775,780 (henceforth, Muttik '780"). The Examiner's rejection is respectfully traversed.

The arguments presented above that demonstrate the allowability of independent claims 1 and 20 in their present form also demonstrate, *mutatis mutandis*, the allowability of independent claims 11, 16 and 17 in their present form.

**§ 103(a) Rejections – Radatti et al. '540 in view of Szor '290, Schmall and Muttik '780 and further in view of Shipley '236**

The Examiner has rejected claims 2, 6, 7 and 14 under § 103(a) as being unpatentable over Radatti et al. '540 in view of Szor '290, Schmall and Muttik '780 and further in view of Shipley, US Patent No. 6,119,236. The Examiner's rejection is respectfully traversed.

It is demonstrated above that independent claims 1 and 11 are allowable in their present form. It follows that claims 2, 6, 7 and 14 that depend therefrom also are allowable.

**§ 103(a) Rejections – Radatti et al. '540 in view of Szor '290, Schmall and Muttik '780 and further in view of Made '076**

The Examiner has rejected claims 5, 8, 9, 12, 13, 18, 19, 21 and 22 under § 103(a) as being unpatentable over Radatti et al. '540 in view of Szor '290, Schmall and Muttik '780 and further in view of Made, US Patent Application Publication No. 2002/0056076 (henceforth, "Made '076"). The Examiner's rejection is respectfully traversed.

It is demonstrated above that independent claims 1, 11, 17 and 20 are allowable in their present form. It follows that claims 5, 8, 9, 12, 13, 18, 19, 21 and 22 that depend therefrom also are allowable.

**§ 103(a) Rejections – Radatti et al. '540 in view of Szor '290, Schmall, Muttik '780 and Made '076 and further in view of Szor '712**

The Examiner has rejected claims 23-26 under § 103(a) as being unpatentable over Radatti et al. '540 in view of Szor '290, Schmall, Muttik '780 and Made '076 and further in view of Szor, US Patent Application Publication No. 2004/0015712 (henceforth, "Szor '712"). The Examiner's rejection is respectfully traversed.

It is demonstrated above that independent claims 1, 11, 17 and 20 are allowable in their present form. It follows that claims 23-26 that depend therefrom also are allowable.

Claims 23-26 are additionally allowable by virtue of reciting the limitation that the attempt to disassemble is initiated at every offset within the suspicious data.

The Examiner has cited Szor '712 paragraph **0054** as teaching this limitation. Strictly speaking, Szor '712 does not teach disassembly of a suspicious executable file **100** but rather emulation of the execution of file **100**. But even if it is posited for the sake of argument that it would be obvious to substitute disassembly for emulation, it still would not be obvious from Szor '712 to disassemble starting from every offset within suspicious data. In paragraph **0054**, Szor '712 teaches emulation starting from every potential *entry point* in file **100**. "Entry points" are defined by Szor '712 in paragraph **0046**:

> Although one embodiment of the emulation control module **520** selects only certain locations in the file **100** as potential entry points, another embodiment of the module **520** treats every instruction in the file **100**, or every instruction within certain regions of the file **100**, as potential entry points.

In other words, the "entry points" of Szor '712 are at the beginnings of instructions. By contrast, claims 23-26 recite attempting disassembly starting from the beginning of every byte in the suspicious data, even if the byte starts in the middle of an instruction, and even if the byte is not part of an instruction at all. That the unit of "offset" in the above-identified patent application is the byte is clear *e.g.* from page 11 line 8 ("an offset of 2 bytes"). Analyzing suspicious data starting at every byte is not at all obvious from Szor '712. It would make no sense for Szor '712 to start emulation in the middle of a multi-byte instruction.

## Other Amendments to the Claims

An inadvertent lack of antecedent basis in claim 16(a) ("the gateway") has been corrected: "the gateway" has been replaced with "a gateway of the network". Support for this amendment is found in the above-identified patent application as filed at least in gateway **101** of LAN **115** in Figure 1.

In view of the above amendments and remarks it is respectfully submitted that independent claims 1, 11, 16, 17 and 20, and hence dependent claims 2-10, 12-14, 18, 19 and 21-26 are in condition for allowance. Prompt notice of allowance is respectfully and earnestly solicited.

Respectfully submitted,

Mark M. Friedman
Attorney for Applicant
Registration No. 33,883

Date: February 4, 2010